Quickscan nationale veiligheid bij inkoop en aanbesteden

Zo houdt u rekening met nationale veiligheidsrisico's

De Quickscan bestaat uit een beperkt aantal vragen om snel te kunnen bepalen of een opdracht een risico vormt voor de nationale veiligheid, of dat er eventueel nader onderzoek nodig is om dit te bepalen. De Quickscan moet in een zo vroeg mogelijk stadium in het inkoopproces worden uitgevoerd, in ieder geval vóór het verzoek om offerte (bij enkel- of meervoudige onderhandse procedures) of ruim voordat de aankondiging van een opdracht wordt gepubliceerd (bij aanbestedingsprocedures). Zodoende kunnen de nodige maatregelen genomen worden als uit de Quickscan naar voren komt dat er risico's zijn voor de nationale veiligheid. De behoeftestellende partij is verantwoordelijk voor het invullen van de Quickscan.

Toelichting

Nederland heeft een open en vrije markteconomie. De geopolitieke context van de (wereld)economie wordt echter complexer en risicovoller. Denk aan economieën met grote staatsinvloed, ingrijpende technologische ontwikkelingen en geopolitieke spanningen tussen landen. Dit kan risico's met zich meebrengen voor de nationale veiligheid bij de inkoop van goederen en diensten.

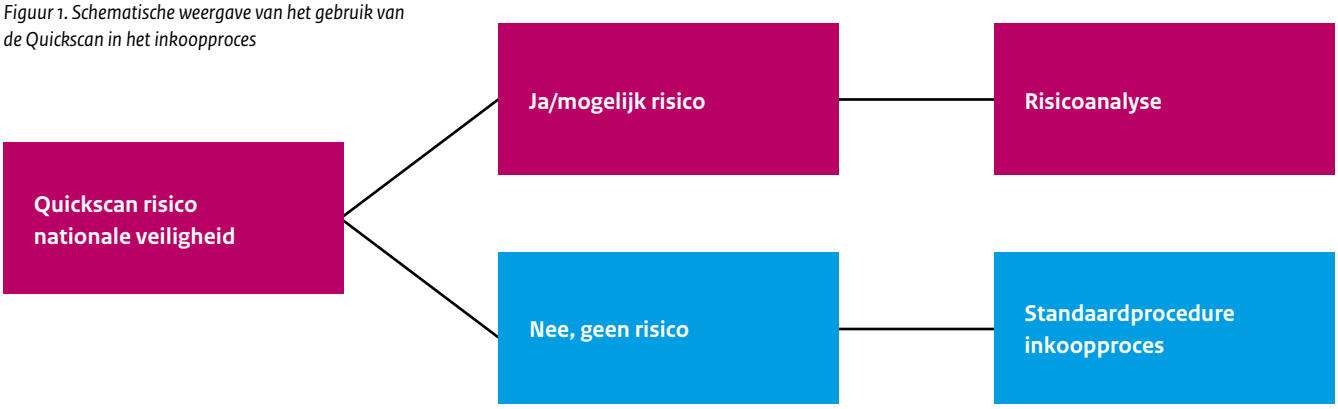
Bij het overgrote deel van de opdrachten zal er geen sprake zijn van een nationale veiligheidsdimensie. Of een opdracht een risico vormt voor de nationale veiligheid hangt sterk af van de sector c.q. het type product of dienst dat geleverd wordt, de opdrachtgever/afnemer en het bedrijf dat de opdracht wordt gegund. In sommige gevallen is het daarom van belang een goede risicoanalyse te maken.
Bij sectoren binnen de vitale infrastructuur treden bijvoorbeeld eerder risico's voor de nationale veiligheid op.

Voorbeelden van nationale veiligheidsrisico's
Bij sommige opdrachten kunnen nationale veiligheidsrisico's aan de orde zijn, bijvoorbeeld:

1. *Verstoring van de continuïteit van de vitale infrastructuur*
   Een opdracht kan ertoe leiden dat de continuïteit van levering, dienstverlening of productie van één van de vitale processen in gevaar komt, denk aan telecommunicatie of energievoorziening. Uitval of verstoring daarvan kan leiden tot ernstige maatschappelijke ontwrichting en vormt een bedreiging voor de nationale veiligheid.
2. *Een strategische afhankelijkheid van partijen en landen met wie Nederland niet dezelfde geopolitieke belangen deelt*
   Een opdracht kan leiden tot een strategische afhankelijkheid van een – al dan niet door een buitenlandse overheid aangestuurde – marktpartij of diens onderaannemers. De afhankelijkheid kan door dat derde land worden misbruikt bijvoorbeeld om politieke druk op Nederland uit te voeren.
3. *Het weglekken van hoogwaardige kennis en vertrouwelijke informatie*
   Het is mogelijk dat voor de uitvoering van een opdracht een opdrachtnemer (of diens onderaannemers) toegang krijgt tot exclusieve kennis en/of vertrouwelijke informatie. Het risico is dan dat vertrouwelijke informatie weglekt. Gegevens kunnen bijvoorbeeld in landen terechtkomen met wetten die het mogelijk maken dat de inlichtingendiensten van deze landen deze kunnen inzien.

Wanneer is het van belang om de Quickscan uit te voeren?
Indien er bij het opstarten van een inkoopproces vermoedens van of twijfels over risico's voor de nationale veiligheid zijn, dient de Quickscan toegepast te worden. De behoeftestellende partij is primair verantwoordelijk voor het beoordelen of er bij een overheidsopdracht mogelijk sprake is van een risico voor de nationale veiligheid. De inkoper is verantwoordelijk voor het vervolgens mitigeren van de mogelijke risico's.

Figuur 1. Schematische weergave van het gebruik van de Quickscan in het inkoopproces



Quickscan

Dit formulier is bedoeld om bij het opstarten van een inkoopproces te beoordelen of er bij de opdracht risico's voor de nationale veiligheid optreden. De Quickscan moet in een zo vroeg mogelijk stadium in het inkoopproces worden uitgevoerd, in ieder geval voor het verzoek om offerte (bij enkel- of meervoudige onderhandse procedures) of ruim voordat de aankondiging van een opdracht wordt gepubliceerd (bij aanbestedingsprocedures), zodat de nodige maatregelen genomen kunnen worden als uit de Quickscan naar voren komt dat er risico's zijn voor de nationale veiligheid. De behoeftestellende partij is verantwoordelijk voor het invullen van de Quickscan.

Quickscan		
		Toelichting
1. Vitale (overheids)processen Raakt de opdracht een vitaal proces? *Zie bijlage 1.1 voor het overzicht van de vitale processen.* *Gaat het bijvoorbeeld om een opdracht voor telecomdiensten, of betreft het een opdracht met betrekking tot de levering van gas? Ook de beschikbaarheid van datasystemen waar meerdere overheidsorganisaties van afhankelijk zijn en communicatie tussen hulpdiensten behoren tot de vitale infrastructuur.*	☐ Ja/Mogelijk ☐ Nee	
2. Strategische afhankelijkheid Ontstaat er door de opdracht een sterke strategische afhankelijkheid van een – al dan niet door een buitenlandse overheid aangestuurde – marktpartij of diens onderaannemers, waardoor bij een conflict de mogelijkheid bestaat dat de opdrachtgever door de opdrachtnemer onder druk kan worden gezet (al dan niet in opdracht van een buitenlandse overheidsactor)? Dit is met name relevant wanneer een product of dienst betrekking heeft op de nationale veiligheid. *Een strategische afhankelijkheid kan bijvoorbeeld ontstaan wanneer de opdracht een product of dienst betreft waarvoor maar weinig opdrachtnemers op de markt beschikbaar zijn, of wanneer plotselinge beëindiging van een levering, bijvoorbeeld door een (statelijk) conflict, tot verstoring leidt in de primaire processen van een organisatie.*	☐ Ja/Mogelijk ☐ Nee	
3. Toegang tot gevoelige informatie Heeft de opdrachtnemer (of diens onderaannemers) toegang nodig tot gevoelige informatie voor het uitvoeren van de opdracht? Denk hierbij aan: • staatsgeheime informatie • informatie die inzicht geeft in de bedrijfsinfrastructuur of ICT infrastructuur waarbij deze informatie van belang kan zijn voor de nationale veiligheid • beschikking over of inzicht in persoonsgegevens (bijvoorbeeld thuisadressen, gegevens bewindspersonen of directe staf bewindspersonen) *Zie bijlage 1.2 voor verdere toelichting over gevoelige informatie*	☐ Ja/Mogelijk ☐ Nee	
4. Toegang tot een gevoelige locatie Krijgt het personeel van de opdrachtnemer (en/of diens onderaannemers) toegang tot fysieke gevoelige locaties van de opdrachtgever? Denk hierbij aan: • Locaties waar gewerkt wordt met staatsgeheime informatie. • Gebouwen van de inlichtingen- en veiligheidsdiensten • Werkplekken van de bewindspersonen	☐ Ja/Mogelijk ☐ Nee	
5. Spionage Ontstaat door de opdracht de mogelijkheid op spionage? Denk bijvoorbeeld aan: • de inhuur van personeel bij de inlichtingen- en veiligheidsdiensten • de inhuur van beveiligingspersoneel • de levering/installatie van printers aan een minister of staatssecretaris	☐ Ja/Mogelijk ☐ Nee	

Indien 'ja/mogelijk' is geantwoord bij één van de voorgaande vragen:

6. Inzet van onderaannemers Ontstaat er bij de uitvoering van de opdracht een situatie, waarin de opdrachtnemer de bevoegdheid heeft nieuwe / andere onderaannemers voor de uitvoering van de opdracht in te zetten?	☐ Ja/Mogelijk ☐ Nee	

CONCLUSIE	
Ja/mogelijk	**Nee**
Indien op *één* van de bovenstaande vragen 'ja/mogelijk' is geantwoord, zijn er mogelijk risico's voor de nationale veiligheid en is een risicoanalyse[1] de volgende stap. In een risicoanalyse wordt uitgebreider stilgestaan bij het identificeren van de risico's voor de nationale veiligheid en wordt gekeken of en hoe risico's kunnen worden gemitigeerd. Denk bijvoorbeeld aan het inbouwen van maatregelen in de selectiefase (selectiecriteria, uitsluitingsgronden, geschiktheidseisen), het kiezen van de juiste procedure of het formuleren van contractvoorwaarden. *Zie bijlage 1.3 voor een indicatie welke risico's zich kunnen voordoen.*	Indien er alleen 'nee' geantwoord is kan het inkoopproces worden voortgezet zonder extra maatregelen in het kader van de nationale veiligheid.

[1] Een handleiding voor de risicoanalyse vindt u hier.

Bijlage Quickscan

1.1 Overzicht vitale processen

De volgende processen zijn in 2018 benoemd als vitaal proces. Voor meer informatie over de vitale infrastructuur en de actuele lijst van vitale processen zie: https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

Vitale processen	Categorie	Sector	Ministerie
Landelijk transport en distributie elektriciteit	A	Energie	EZK
Regionale distributie elektriciteit	B		
Gasproductie, landelijk transport en distributie gas	A		
Regionale distributie gas	B		
Olievoorziening	A		
Internet en datadiensten	B	ICT/Telecom	EZK
Internettoegang en dataverkeer	B		
Spraakdienst en SMS	B		
Plaats- en tijdsbepaling middels GPS	B		IenW
Drinkwatervoorziening	A	Drinkwater	IenW
Keren en beheren waterkwantiteit	A	Water	IenW
Vlucht- en vliegtuigafhandeling	B	Transport	IenW
Scheepvaartafwikkeling	B		
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	B	Chemie	IenW
Opslag, productie en verwerking nucleair materiaal	A	Nucleair	IenW
Toonbankbetalingsverkeer	B	Financieel	FIN
Massaal giraal betalingsverkeer	B		
Hoogwaardig betalingsverkeer tussen banken	B		
Effectenverkeer	B		
Communicatie met en tussen hulpdiensten middels 112 en C2000	B	OOV	JenV
Inzet politie	B		
Basisregistraties personen en organisaties	B	Digitale overheids-processen	BZK
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)	B		
Elektronisch berichtenverkeer en informatieverschaffing aan burgers	B		
Identificatie en authenticatie van burgers en bedrijven	B		
Inzet defensie	B	Defensie	DEF

1.2 Gevoelige informatie

Er bestaan verschillende kwalificaties van het begrip gevoelige informatie. Gevoelige informatie ziet niet alleen toe op staatsgeheime (Stg.) informatie, maar ook op informatie die op het eerste oog minder belangrijk lijkt te zijn maar voor een kwaadwillende partij toch interessant kan zijn.

1. *Bijzondere informatie* is informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries[2]. Bijzondere informatie bestaat in verschillende gradaties:
   - Stg. ZEER GEHEIM, Stg. GEHEIM en Stg. CONFIDENTIEEL
     Voor alle drie geldt dat kennisname door niet-geautoriseerden schade kan toebrengen aan één van de vitale belangen van de Staat of zijn bondgenoten (denk aan de notulen van de ministerraad)
   - Dep. VERTROUWELIJK
     Kennisname door niet-geautoriseerden kan schade toebrengen aan de belangen van één of meer ministeries (bijvoorbeeld verslagen bestuursraad of codeberichten van het ministerie van buitenlandse zaken).

2. In het privaatrechtelijk domein wordt de aanduiding *vertrouwelijke informatie* als volgt gebruikt: Informatie die door een contractspartij in vertrouwen of onder voorwaarden aan een overheidsinstelling beschikbaar is gesteld, wordt over het algemeen contractueel beschermd tegen ongewenste verspreiding.
   Te denken valt aan bedrijfsvertrouwelijke informatie, of documenten waarop intellectueel eigendom van toepassing is.

3. *Strategische informatie:* Ook informatie die niet als gerubriceerd is aangemerkt, kan van strategisch belang zijn. Als deze informatie ongewenst in verkeerde handen valt en/of ertoe kan leiden dat derden inzage krijgen in de werking van de overheid. Denk aan de paraatheid van het leger door informatie over verschillende locaties of meer inzicht in de werking van organisaties die vitale diensten leveren.

4. *Persoonsgegevens* zijn een bijzondere verschijningsvorm van informatie. Persoonsgegevens (zeker grote bestanden) kunnen interessant zijn voor kwaadwillende partijen. Denk bijvoorbeeld aan de huisadressen van bewindspersonen of de contactgegevens van werknemers van de veiligheidsdiensten. De Algemene verordening gegevensbescherming (AVG) geeft het kader waarbinnen het beschikbaar stellen en verwerken van deze vorm van informatie juridisch als toegestaan mag worden beschouwd.

1.3 Risicoanalyse: op welk gebied kunnen zich risico's voordoen?

Bij een risicoanalyse kan gekeken worden naar de nationale veiligheidsbelangen, de mogelijke risico's (en op welk gebied die zich voordoen) en met welke maatregelen in het inkoopproces deze mogelijke risico's kunnen worden beheerst. Op basis van de risicoanalyse kan vervolgens bepaald worden of risico's niet voldoende beheersbaar zijn en of het wenselijk is dat de opdracht door een marktpartij wordt uitgevoerd. Als wordt geconcludeerd dat de opdracht wel aan de markt wordt aangeboden, kunnen op basis van de risicoanalyse maatregelen genomen worden op het gebied van de te volgen procedure, de selectie- en geschiktheidseisen en de contractuele voorwaarden.

Om de risico's goed te kunnen inschatten is het van belang vóóraf inzicht te krijgen in potentiele opdrachtnemers. Risico's kunnen zich voordoen op verschillende gebieden:

1. *Het bestuur en de organisatie van de te contracteren opdrachtnemer*
   - Kenmerken van de opdrachtnemer, wijzigingen in aandeelhouderschap, eigendom of zeggenschap in diens rechtspersoon, of de samenstelling van de logistieke toeleveringsketen, kunnen van invloed zijn op in de opdracht aanwezige gevoelige informatie. Indien aanwezige risico's op dit gebied niet voldoende zijn afgedekt, kan er een strategische afhankelijkheid van een opdrachtnemer ontstaan.
   - Is de organisatie wel ingericht op de informatie waar ze mee moeten werken? Weten ze wat ze moeten doen als beveiligingsincidenten zich voordoen en voldoen ook de onderaannemers aan de beveiligingseisen voor de opdracht? Indien dit niet het geval is, kan er tijdens de contractperiode eerder gevoelige informatie weglekken.
   - Op het gebied van het bestuur en de organisatie van de opdrachtnemer kunnen er verder risico's ontstaan als het bedrijf openlijk of verborgen wordt gestuurd door een staat, waardoor via het bedrijf de geopolitieke, strategische en economische macht vergroot kan worden. In sommige landen is het in de wet verankerd dat er informatie gedeeld moet worden met de inlichtingen- en veiligheidsdiensten. Door de samenwerking met een dergelijk bedrijf aan te gaan, kan een strategische afhankelijkheid ontstaan, kan informatie weglekken, of kan de continuïteit van levering in gevaar komen.
   - Indien bovenstaande niet van toepassing is op de toekomstige contractpartij, betekent het niet dat er geen risico meer kan ontstaan. De organisatie kan bijvoorbeeld tijdens de contractperiode worden overgenomen, of de bestuurders kunnen wisselen. Denk ook aan een bedrijfsbeëindiging, wisseling in onderaannemers of een faillissement.

[2] Zie: Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) http://wetten.overheid.nl/BWBR0033507/2013-06-01

2. *De inzet van personeel*
   Als personeel in aanraking komen met gevoelige informatie is het noodzakelijk dat betrouwbaarheidseisen worden gesteld. Dit geldt zowel voor het eigen personeel van opdrachtgever als voor het personeel van opdrachtnemer (en diens logistieke toeleveringsketen). Als hier geen afspraken over worden gemaakt kan het voorkomen dat personeel zonder vertrouwensfunctie (op het juiste niveau gescreend) met vertrouwelijke informatie gaat werken. Of als vertrouwensfuncties ook open staan voor buitenlandse kandidaten is het de vraag of het screeningsniveau voldoende kunnen worden gegarandeerd. En wat gebeurt er met de informatie na beëindiging van het contract? Ook als er geen sanctie-instrumentarium op zijn plaats is met betrekking tot de overtreding van beveiligingsregels, is het aan te bevelen om hier afspraken over te maken.

3. *Fysieke beveiliging*
   Als op de eigen locatie van de opdrachtnemer sprake is van opslag, verwerking of transport met betrekking tot de opdracht, al dan niet in een daartoe aangewezen compartiment op die locatie (bijvoorbeeld een fysieke ruimte in een gebouw), zal die locatie c.q. het compartiment fysiek beveiligd moeten worden. Maatregelen rondom fysieke toegang moeten onrechtmatige toegang onmogelijk maken, en pogingen daartoe in elk geval tijdig signaleren (registratie, pascontrole enz.). Daarbij gaat het om de fysieke locatie, waar gewerkt wordt met/aan de opdracht, om de locatie waar informatie over de opdracht wordt opgeslagen, en om de locatie waar over de opdracht wordt gesproken.
   Als hier geen afspraken over gemaakt worden is het risico dat niet-geautoriseerd personeel of bezoekers toegang heeft tot de gevoelige locaties en informatie en dat deze informatie kan weglekken.

4. *Digitale weerbaarheid*
   Naast fysieke beveiliging is digitale weerbaarheid ook van belang en kan informatie in verkeerde handen komen als er geen beleid is rondom cybersecurity of er geen toezicht op een veilige inrichting van de digitale infrastructuur wordt gehouden. Als dit niet regelmatig getoetst/geaudit wordt, is het bovendien de vraag of hier gedurende de contractperiode voldoende aandacht aan wordt besteed. Ook op dit gebied is het aan te raden om eisen te stellen en afspraken te maken.

Meer informatie:

Rijksportaal - Nationale veiligheid bij inkoop en aanbesteden

VeiligInkopen@minbzk.nl

Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,
in samenwerking met de Nationaal Coördinator
Terrorismebestrijding en Veiligheid

November 2018 | 117631